UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

NICK THWEATT, individually and on behalf of all others similarly situated, Plaintiff, v. LENOVO (UNITED STATES) INC., LENOVO GROUP LIMITED, and SUPERFISH, INC., Defendants.	No. C15-390 **COMPLAINT – CLASS ACTION** **DEMAND FOR JURY TRIAL**

Nick Thweatt ("Plaintiff"), individually and on behalf of all others similarly situated, by his attorneys, makes the following allegations and claims against Lenovo (United States) Inc., Lenovo Group Limited (together referred to as "Lenovo"), and Superfish, Inc. ("Superfish"). These allegations are made upon information and belief except as to allegations specifically pertaining to Plaintiff, which are made upon knowledge.

NATURE OF THE ACTION

1. This is a consumer class action brought by Plaintiff on behalf of himself and all others similarly situated in the United States of America who have purchased certain models of

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

computers manufactured and marketed by Lenovo that were pre-installed with spyware and/malware called Superfish from at least September 2014 through February 2015 (the "Relevant Period"). Superfish, among other actions, monitors, intercepts, analyzes and redirect users' web activity and personal information and tampers with Windows' security system to procure advertising into secure pages. As a result, users of these computers were exposed to potential computer hackers and unauthorized activity monitoring.

PARTIES

2. Plaintiff Nick Thweatt is an individual residing in Lynden, Washington. Plaintiff bought a YOGA2-11 Lenovo computer in November 2014 from Best Buy.

3. Defendant Lenovo (United States) Inc. ("Lenovo US") is a Delaware corporation with its headquarters at 1009 Think Place, Morrisville, North Carolina 27560.

4. Defendant Lenovo Group Limited ("Lenovo Group") is a Hong Kong Corporation with its headquarters at Shangdi Information Industry Base, No 6 Chuang Ye Road, Haidian District, 100085 Beijing, China. Lenovo Group is the parent company of Lenovo US.

5. Defendants Lenovo US and Lenovo Group are collectively referred to as "Lenovo" in this Complaint.

6. Defendant Superfish, Inc. is a Delaware corporation with its headquarters located at 2595 East Bayshore Road, Palo Alto, California 94303.

JURISDICTION AND VENUE

7. This Court has federal-question jurisdiction under 28 U.S.C. § 1331. Plaintiff states federal statutory claims under the Federal Wiretap Act (Title 1 of the ECPA, 18 U.S.C. § 2510 et seq.), the Stored Communications Act ("SCA") (18 U.S.C. § 2701, et seq.), and the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

8. This Court also has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). Plaintiff's claims and the claims of the other members of the class exceed $5,000,000, exclusive of interests and costs, and at least one class member is a citizen of a state different from the Defendants' states of citizenship.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

9. This Court has supplemental jurisdiction over the related state law claims under 28 U.S.C. § 1367(a) because they form part of the same case or controversy under Article III of the U.S. Constitution and the state law claims are derived from a common nucleus of operative facts such that the parties would ordinarily expect to try them in one judicial proceeding.

10. This Court has personal jurisdiction over Defendants because Defendants conduct business in Washington and Defendants Lenovo US and Superfish may be served here.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Plaintiff resides in this District. Also, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District. And, Defendants Lenovo US and Superfish maintain registered agents in this District and may be served here.

COMMON FACTUAL ALLEGATIONS

12. Lenovo is a computer technology company that designs, develops, and manufactures various computer and technological products such as laptops, tablets, desktops, all-in-ones, and workstations. According to its website, Lenovo is the world's largest PC vendor and fourth largest smartphone company. Lenovo is a $39 billion company with more than 54,000 employees in more than 60 countries serving customers in more than 160 countries. Lenovo US is the subsidiary of Lenovo Group.

13. Beginning in September 2014, Lenovo pre-installed Superfish VisualDiscovery spyware on some of its computers before selling those computers to the public.

14. A security expert, Marc Rogers, published a blog post on February 19, 2015 titled "*Lenovo Installs Adware on Customer Laptops and Compromises all SSL*." Mr. Rogers detailed the invasive features of Superfish and the potential damage it can cause. The article can be accessed at http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/. His blog stated in part:

Superfish Features:

- Hijacks legitimate connections
- Monitors user activity

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

- Collects personal information and uploads it to its servers
- Injects advertising in legitimate pages
- Displays popups with advertising software
- Uses man-in-the-middle attack techniques to crack open secure connections
- Presents users with its own fake certificate instead of the legitimate site's certificate.

This presents a security nightmare for affected consumers.

1. Superfish replaces legitimate site certificates with its own in order to compromise the connections so it can inject its adverts. This means that anyone affected by this adware cannot trust any secure connections they make.
2. Users will not be notified if the legitimate site's certificate has been tampered with, has expired, or is bogus. In fact, they now have to rely on Superfish to perform that check for them. Which it does not appear to do.
3. Because Superfish uses the same certificate for every site, it would be easy for another hostile actor to leverage this and further compromise the user's connections.
4. Superfish uses a deprecated SHA1 certificate. SHA1 has been replaced by SHA-256 because attacks against SHA1 are now feasible with ordinary computing hardware. This is insult on top of injury. Not only are they compromising people's SSL connections but they are doing it in the most cavalier, insecure way possible.
5. Even worse, they use crackable 1024-bit RSA!
6. The user has to trust that this software which has compromised their secure connections is not tampering with the content or stealing sensitive data such as usernames and passwords.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

7. If this software or any of its control infrastructure is compromised, an attacker would have complete and unrestricted access to affected customers' banking sites, personal data, and private messages.

15. Windows Ecosystem Vice President Mark Cohen told InfoWorld that "Lenovo had screened the software from Superfish before it was installed on Lenovo's consumer laptop lines" and "had asked Superfish to remove certain features that abused SSL connections."

16. Customer complaints began almost immediately. On January 23, 2015, Lenovo admitted that it had installed Superfish software on various computers and that it would no longer install the software on future products. Lenovo, however, did not make any efforts to remove the software on existing products or help pay for customers to remove of the damaging software.

17. On February 19, 2015, Lenovo issued a press release on its website titled "Lenovo Statement on Superfish." Lenovo admitted that it had pre-installed Superfish on some of its computers and that its goal "was to improve the shopping experience using their visual discovery techniques." Lenovo also stated in the press release that it had customer complaints about the software.

18. In this press release, there was a link to a description of Superfish. The page stated that "Superfish intercepts HTTP(s) traffic using a self-signed root certificate. This is stored in the local certificate store and provides a security concern." Here, Lenovo admitted to wiretapping communications and admitted that, by pre-installing Superfish on its computers, customers were vulnerable to attack.

19. In addition, Lenovo listed the make and models of computers that may have had Superfish installed. The makes and models listed are as follows:

G Series: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, G40-80

U Series: U330P, U430P, U330Touch, U430Touch, U530Touch

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

Y Series: Y430P, Y40-70, Y50-70, Y40-80, Y70-70

Z Series: Z40-75, Z50-75, Z40-70, Z50-70, Z70-80

S Series: S310, S410, S40-70, S415, S415Touch, S435, S20-30, S20-30Touch

Flex Series: Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 Pro, Flex 10

MIIX Series: MIIX2-8, MIIX2-10, MIIX2-11, MIIX 3 1030

YOGA Series: YOGA2Pro-13, YOGA2-13, YOGA2-11, YOGA3 Pro

E Series: E10-30

Edge Series: Lenovo Edge 15

20. The same day, an article was published on Bloomberg.com titled "*Lenovo Apologizes After It 'Messed Up' With Tracking Software*" by Jordan Roberson. The article can be accessed at http://www.bloomberg.com/news/articles/2015-02-19/lenovo-says-it-messed-up-by-preloading-web-tracking-software. The article stated in part:

> "**We messed up badly here**," Peter Hortensius, Lenovo's chief technology officer, said in an interview. "**We made a mistake. Our guys missed it. We're not trying to hide from the issue – we're owning it**."

21. Another article was published on February 19th on *eff.com* titled "*Lenovo is Breaking HTTPS Security on its Recent Laptops*" by Joseph Bonneau, Peter Eckersley, and Jacob Hoffman-Andrews. The article can be accessed at https://www.eff.com/es/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops. The article stated in part:

> Lenovo has not just injected ads in a wildly inappropriate manner, but engineered a **massive security catastrophe** for its users. The use of a single certificate for all of the MITM attacks means that *all* HTTPS security for at least Internet Explorer, Chrome, and Safari for Windows, on *all* of these Lenovo laptops, is now broken. If you access your webmail from such a laptop, any network attacker can read your mail as well or steal your password. If you log into your online banking

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

> account, any network attacker can pilfer your credentials. All an attacker needs in order to perform these attacks is a copy of the Superfish MITM private key.
>
> Using a MITM certificate to inject ads **was an amateurish design choice** by Superfish. Lenovo's decision to ship this software **was catastrophically irresponsible and an utter abuse of the trust** their customers placed in them.

22. On February 20, 2015, the United States Computer Emergency Readiness Team, a division of the United States Department of Homeland Security, issued an alert titled "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing." The alert gave a description of the problem and stated that its impact was "a machine with Superfish VisualDiscovery installed will be vulnerable to SSL spoofing attacks without a warning from the browser." The alert further stated that users should uninstall spyware along with removing the affected root CA certificates.

PLAINTIFF'S FACTUAL ALLEGATIONS

23. Plaintiff bought a YOGA2-11 Lenovo computer in November 2014. Unknown to Plaintiff at the time of purchase, the computer had Superfish spyware software pre-installed on it.

24. As a result of the Superfish spyware, Plaintiff had issues with his PayPal account, including fraudulent charges and fraudulent website logon attempts.

25. Plaintiff used the computer for online personal and business banking. He also used the computer to make online credit card purchases. Plaintiff ran the removal tool released by Lenovo on February 22, 2015.

CLASS ACTION ALLEGATIONS

26. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Fed. R. Civ. P. 23. Plaintiff seeks to represent a class (the "Class") described as follows:

> All individuals and entities in the United States who purchased a Lenovo computer with the Superfish Surveillance Software preinstalled on it and who connected the computer to the internet.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

27. The members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact numbers of Class members is unknown to Plaintiff at this time, it is believed to be in the millions.

28. This action satisfies the commonality and predominance requirements of Fed. R. Civ. P. 23(a) and (b)(3) because it involves questions of law and fact common to the members of the Class that predominate over any questions affecting only individual members, including but not limited to:

(a) Whether Defendants violated the Federal Wiretap Act, Title I of the ECPA (18 U.S.C. §§ 2510 *et seq.*);

(b) Whether Defendants violated the Stored Communications Act, Title II of the ECPA (18 U.S.C. §§ 2701 *et seq.*);

(c) Whether Defendants violated the Computer Fraud and Abuse Act (18 U.S.C. §1030);

(d) Whether Defendants violated the Washington Consumer Protection Act (RCW § 19.86.010 et seq.);

(e) Whether Defendants committed the tort of invasion of privacy;

(f) Whether Defendants committed the tort of trespass to chattels;

(g) Whether Defendants were unjustly enriched;

(h) Whether Plaintiff and members of the Class have been injured by Defendants' conduct;

(k) Whether Plaintiff and the Class are entitled to damages, statutory damages, treble damages, and/or equitable, injunctive, or declaratory relief.

29. Plaintiff's claims are typical of those of other Class members because Plaintiff's computer was infected with Superfish, like that of every Class member.

30. Plaintiff will fairly and adequately represent and protect the interests of the Class.

31. Plaintiff's counsel is competent and experienced in class action litigation.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

32. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Class members is not practicable, and questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the proposed Class.

33. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Lenovo and Superfish and would lead to repetitive adjudication of common questions of law and fact.

34. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class certification, Lenovo's and Superfish's violations of law would go unremedied and Lenovo and Superfish will retain the benefits of their wrongdoing.

35. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

36. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Lenovo and Superfish have acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

VIOLATION OF THE FEDERAL WIRETAP ACT

(Title I of the ECPA, 18. U.S.C. §§ 2510 et seq.)

37. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

38. Under the Federal Wiretap Act, a plaintiff has a private cause of action. The statute states "any person whose wire, oral, or electronic communication is intercepted,

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a).

39. "Electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

40. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

41. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

42. Under 18 U.S.C. § 2511(1)(a), it is illegal when a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

43. Plaintiff and Class members are persons as defined under 18 U.S.C. § 2510(6).

44. Defendants Lenovo and Superfish are corporations and therefore persons as defined under 18 U.S.C. § 2510(6).

45. Defendants intentionally intercepted and endeavored to intercept Plaintiff's and Class members' electronic communications, without their knowledge or consent, in violation of the Act.

46. Under 18 U.S.C. § 2520, Plaintiff seeks preliminary, equitable, and declaratory relief; actual damages or statutory damages, whichever is greater; punitive damages to the extent available; and reasonable attorneys' fees and costs.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

COUNT II

VIOLATION OF THE STORED COMMUNICATIONS ACT

(Title II of the ECPA, 18 U.S.C. § 2701 et seq.)

47. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

48. Under the Stored Communications Act, a plaintiff has a private cause of action. The statute states "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2707(a).

49. Under the Act, it is unlawful for a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentional exceeds an authorization to access that facility" and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system…" 18 U.S.C. § 2701(a).

50. "Electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

51. "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

52. Defendants intentionally intercepted Plaintiff's communications while they were in storage. In addition, Defendants accessed the content of the Plaintiff's stored communications without authorization or exceeded its authorization from any party to the communications.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

53. Under 18 U.S.C. § 2707(c), Plaintiff seeks statutory damages of no less than $1,000; punitive damages to the extent available, and reasonable attorneys' fees and costs.

COUNT III

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

(18 U.S.C. § 1030)

54. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

55. Under the Computer Fraud and Abuse Act, a plaintiff has a private cause of action. Under the Act, "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). The conduct must involve "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related court of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

56. Under the Act, it is illegal for a person who "intentionally accesses a computer without authorization or exceeds access, and thereby obtains…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

57. "Protected computer" means a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

58. The Plaintiff's and Class Members' computers were used in interstate commerce and therefore were protected computers as defined under the Act.

59. Defendants intentionally accessed the Plaintiff's and Class Members' computers without authorization or exceeded access to the computers, and obtained information from the

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

protected computers. On information and belief, the aggregate loss resulting from Defendants' conduct in violation of this Act exceeds $5,000 during a 1-year period.

60. Under 18 U.S.C. § 1030(g), Plaintiff seeks compensatory damages, injunctive relief, and other equitable relief. Plaintiff also seeks reasonable attorneys' fees and costs.

COUNT IV

VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT

(RCW § 19.86.010 et seq.)

Against Defendant Lenovo

61. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

62. The purpose of Washington's Consumer Protection Act, RCW § 19.86.010 et seq. ("CPA"), is "to protect the public and foster fair and honest competition …" The act is "liberally construed" to serve its beneficial purposes. RCW § 19.86.920.

63. To achieve its goals, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce ..." RCW § 19.86.020.

64. The CPA prohibits (a) an unfair or deceptive act or practice, (b) occurring in trade or commerce, (c) with a public interest impact, (d) that causes injury.

65. In the context of the CPA, pleading and proof of an unfair or deceptive act or practice under RCW § 19.86.020 bears little resemblance to pleading and proof of common-law fraud. It can be predicated on an act or practice that has the capacity to deceive the public; or an unfair or deceptive act or practice not regulated by statute but in violation of public interest. An act or practice can be unfair without being deceptive and still violate the CPA.

66. Defendants, by marketing computers to the public with spyware pre-installed and then using that spyware to obtain information about users and disrupt the ordinary functioning of the computers, including security features, engaged in secret and damaging conduct that Defendants did not disclose and reasonable users did not and would not expect.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

67. Defendants' wrongdoing was both unfair and deceptive within the meaning of the CPA.

68. Defendants' wrongful practices occurred in the conduct of trade or commerce.

69. Defendants' wrongful practices were and are injurious to the public interest because those practices were part of a pattern or generalized course of conduct on the part of Defendants and were repeated continuously before and after Plaintiff bought and used his Lenovo computer. Many users in Washington state have been adversely affected by Defendants' conduct and the public was and is at risk.

70. As a result of Defendants' conduct, Plaintiff and the Class members were injured in their business or property – i.e., economic injury – in that they were charged and paid for a computer with embedded spyware that was worth substantially less than a computer without that same spyware; and the spyware continued to cause economic injury to Plaintiff and the Class members as they used their computers to access the Internet.

71. Defendants' unfair and/or deceptive conduct proximately caused Plaintiff's and the Class members' injury because, had Defendants disclosed that their computers were infected, Plaintiff and the Class members would have paid less for them; and had the computers not been infected, Plaintiff and the Class members would not have suffered harm because Defendants would not have been able to secretly abscond with their private information and affect the computers' security features.

72. Plaintiff, individually and on behalf of the Class, seeks to enjoin further violations of the CPA and recover actual and treble damages, together with the costs of suit including reasonable attorneys' fees.

COUNT V

INVASION OF PRIVACY

73. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

74. Plaintiff and the Class had an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential, personally identifiable information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including but not limited to the right to visit and interact with various internet sites without having that information intercepted and transmitted to Defendants without knowledge or consent.

75. Plaintiff and the Class had a reasonable expectation that their personally identifiable information and other data would remain confidential and that Defendants would not install spyware on their computers that would enable Defendants to track their activities on the internet or intercept emails.

76. This invasion of privacy is serious in nature, scope, and impact.

77. This invasion of privacy constitutes an egregious breach of the social norms underlying the privacy right and caused harm to Plaintiff and the Class.

COUNT VI

TRESPASS TO CHATTELS

78. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

79. Defendants, intentionally and without consent or other legal justification, placed malicious spyware on Plaintiff's and the Class's computers which intercepted and altered their communications and also rendered their computer vulnerable to attack.

80. Defendants, intentionally and without consent or other legal justification, through their malicious spyware, caused actual damages.

81. Defendants' intentional and unjustified placing of malicious spyware and interception and alteration of communications interfered with Plaintiff's and the Class's use of their computers.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

COUNT VII

UNJUST ENRICHMENT

82. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

83. Plaintiff and the Class conferred a monetary benefit on Lenovo and Superfish in the form of monies paid for the purchase of computers from Lenovo and information that Defendants wrongfully obtained and monetized from Plaintiff and the Class.

84. Defendants appreciate or have knowledge of the benefits conferred directly upon them by Plaintiff and members of the Class.

85. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and members of the Class.

86. Plaintiff and the Class have conferred directly upon Defendants an economic benefit in the nature of monies received and profits resulting from sales to the economic detriment of Plaintiff and the Class members.

87. The economic benefit, including the monies paid and profits derived by Defendants and paid by Plaintiff and members of the Class, is a direct and proximate result of Defendants' unlawful practices as set forth in this Complaint.

88. The financial benefits derived by Defendants rightfully belong to Plaintiff and members of the Class.

89. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and the Class.

90. Plaintiff and the Class have no adequate remedy at law.

COUNT VIII

DECLARATORY RELIEF

(28 U.S.C. § 2201)

91. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

92. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendants for which Plaintiff desires a declaration of rights.

93. Plaintiff contends that Defendants' acts, practices, and conduct violate various federal and state privacy and unfair competition laws, as alleged herein.

94. Plaintiff, on behalf of himself and the Class, is entitled to a declaration that Defendants violated the federal and state statutes and state common law alleged herein.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Class, requests that the Court enter judgment against Defendants and enter an order:

A. certifying this case as a class action under Fed. R. Civ. P. 23(a), (b)(2) and (b)(3); and appoint Plaintiff to be Class representative and his undersigned counsel to be Class counsel;

B. requiring Defendants to make whole any losses suffered by Plaintiff and Class members;

C. enjoining Defendants from further engaging in the unlawful conduct complained of herein;

D. requiring Defendants to collect and destroy all data they wrongfully obtained from Plaintiff and the Class;

E. awarding Plaintiff and the Class appropriate relief, including actual and statutory damages, treble damages, restitution, and disgorgement;

F. awarding pre-judgment and post-judgment interest, to the extent allowable;

G. requiring Defendants to pay for notifying the Class of the pendency of this action;

H. requiring Defendants to pay Plaintiff and Class members reasonable attorneys' fees, expenses, and the costs of this action; and

I. providing all other relief as this Court deems necessary, just, and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

LAW OFFICES OF
CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074-7033
Tel: (425) 868-7813 • Fax: (425) 732-3752

Dated: March 13, 2015

Respectfully submitted,

s/ *Cliff Cantor*
By: Cliff Cantor, WSBA # 17893
LAW OFFICES OF CLIFFORD A. CANTOR, P.C.
627 208th Ave. SE
Sammamish, WA 98074
Tel: (425) 868-7813
Fax: (425) 732-3752
Email: cliff.cantor@outlook.com

William B. Federman *
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Tel: (405) 235-1560
Fax: (405) 239-2112
Email: wbf@federmanlaw.com

* to apply for admission pro hac vice

Attorneys for Plaintiff Nick Thweatt and the Class